Conclusive Entangling Probe

Howard E. Brandt
U.S. Army Research Laboratory, Adelphi, MD
hbrandt@arl.army.mil

February 1, 2008

Abstract

A design is given for an optimized entangling probe attacking the BB84 (Bennett-Brassard 1984) protocol of quantum key distribution and yielding maximum information to the probe for a full range of induced error rates. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. Although standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key, if instead the probe measurements are performed with a certain positive operator valued measure, then the measurement results are conclusive, at least some of the time, for a full range of inconclusive rates.

Keywords: quantum cryptography, quantum key distribution, quantum communication, entanglement.

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ta

1 INTRODUCTION

Recently, a design was presented [1], [2] for an optimized entangling probe attacking the BB84 Protocol [3] of quantum key distribution (QKD) and yielding maximum information to the probe. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. Although standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key, it was shown that if instead the probe measurements are performed with a certain positive operator valued measure (POVM) [4], [5], [6] [7], [8] then the measurement results are conclusive, at least some of the time [9]. If the inconclusive rate equals the loss rate of the legitimate receiver (due to attenuation in the key distribution channel), and only the unambiguous states are relayed by the probe to the legitimate receiver, then the probe can obtain complete information on the pre-privacy amplified key, once the bases are announced on the public channel during reconciliation. The implementation in [1], [2] applied for error rates less than 1/4, thereby allowing inconclusive rates of the POVM

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **01 FEB 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Conclusive Entangling Probe**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory,Adelphi,MD**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A design is given for an optimized entangling probe attacking the BB84 (Bennett-Brassard 1984) protocol of quantum key distribution and yielding maximum information to the probe for a full range of induced error rates. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. Although standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key if instead the probe measurements are performed with a certain positive operator valued measure, then the measurement results are conclusive, at least some of the time, for a full range of inconclusive rates.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

receiver exceeding 1/3. In the present work, an alternative probe design is presented for which the error rate is less than 1/3. This enables an inconclusive rate of the POVM receiver ranging from 0 to 1, matching possible loss rates between the probe and the legitimate receiver.

In Section 2, the alternative optimized unitary transformation is reviewed, representing the action of an optimized entangling probe yielding maximum information on quantum key distribution in the BB84 protocol. In Section 3, the design is given of the entangling probe for a full range of induced error rates. In Section 4, analysis is presented for alternatively using the POVM receiver of [4] to measure the probe, thereby unambiguously discriminating the signal, at least some of the time. Section 5 contains a summary.

2 ALTERNATIVE ENTANGLING PROBE

In the present work, I present an implementation of the optimum unitary transformation given by Eqs.(158)-(164) of [1], however with restricted parameters such that the corresponding Hilbert space of the probe reduces from four to two dimensions. In particular, the parameters μ and θ are here restricted to

$$\sin\mu = \cos\mu = 2^{-1/2}, \qquad \cos\theta = 1. \tag{1}$$

In this case, the entangling probe states $|\sigma_+\rangle$, $|\sigma_-\rangle$, $|\sigma\rangle$, $|\delta_+\rangle$, $|\delta_-\rangle$, $|\delta\rangle$, given by Eqs. (159)-(164) of [1], become

$$|\sigma_+\rangle = |\delta_-\rangle = 4[(1-2E)^{1/2}\,|w_a\rangle - E^{1/2}\,|w_b\rangle], \tag{2}$$

$$|\sigma_-\rangle = |\delta_+\rangle = 4[(1-2E)^{1/2}\,|w_a\rangle + E^{1/2}\,|w_b\rangle], \tag{3}$$

$$|\sigma\rangle = -\,|\delta\rangle = 4E^{1/2}\,|w_b\rangle\,, \tag{4}$$

in which I have made the upper sign choices in Eqs.(159)-(164) of [1], E is the error rate induced by the probe, and the orthonormal probe basis vectors $|w_a\rangle$ and $|w_b\rangle$ are defined by

$$|w_a\rangle = 2^{-1/2}\,(|w_0\rangle + |w_3\rangle)\,, \tag{5}$$

$$|w_b\rangle = 2^{-1/2}\,(|w_1\rangle - |w_2\rangle)\,, \tag{6}$$

expressed in terms of the orthonormal basis vectors $|w_0\rangle$, $|w_3\rangle$, $|w_1\rangle$, and $|w_2\rangle$ of [1]. Thus, the optimum unitary transformation, Eq.(158) of [1], produces in this case the following entanglements for initial probe state $|w\rangle$ and incoming BB84 signal photon-polarization states $|u\rangle$, $|\bar{u}\rangle$, $|v\rangle$, or $|\bar{v}\rangle$, respectively:

$$|u\rangle \otimes |w\rangle \longrightarrow \frac{1}{4}\,(|u\rangle \otimes |\sigma_+\rangle + |\bar{u}\rangle \otimes |\sigma\rangle)\,, \tag{7}$$

$$|\bar{u}\rangle \otimes |w\rangle \longrightarrow \frac{1}{4}\left(|u\rangle \otimes |\sigma\rangle + |\bar{u}\rangle \otimes |\sigma_-\rangle\right), \tag{8}$$

$$|v\rangle \otimes |w\rangle \longrightarrow \frac{1}{4}\left(|v\rangle \otimes |\sigma_-\rangle - |\bar{v}\rangle \otimes |\sigma\rangle\right), \tag{9}$$

$$|\bar{v}\rangle \otimes |w\rangle \longrightarrow \frac{1}{4}\left(-|v\rangle \otimes |\sigma\rangle + |\bar{v}\rangle \otimes |\sigma_+\rangle\right). \tag{10}$$

Here, the probe states $|\sigma_+\rangle$, $|\sigma_-\rangle$, $|\sigma\rangle$ are given by Eqs.(2)-(4). The states $|u\rangle$ and $|\bar{u}\rangle$ are orthogonal linearly-polarized photon signal states in the $\{|u\rangle, |\bar{u}\rangle\}$ basis, and $|v\rangle$ and $|\bar{v}\rangle$ are orthogonal linearly-polarized photon signal states in the $\{|v\rangle, |\bar{v}\rangle\}$ basis, and the two bases are nonorthogonal with $\pi/4$ angle between the linear polarizations of states $|u\rangle$ and $|v\rangle$. In the present case, the maximum information gain by the probe is again given by

$$I_{opt}^{R} = \log_2\left[2 - \left(\frac{1-3E}{1-E}\right)^2\right], \tag{11}$$

and here $E \leq 1/3$, since $E = 1/3$ corresponds to perfect information.

3 DESIGN OF ENTANGLING PROBE

Using the same methods presented in [1], it can be shown that a quantum circuit consisting again of a single CNOT gate suffices to produce the optimum entanglement, Eqs.(7)-(10). Here, the control qubit entering the control port of the CNOT gate consists of the two signal basis states $\{|e_0\rangle, |e_1\rangle\}$. In the two-dimensional Hilbert space of the signal, the basis states $|e_0\rangle$ and $|e_1\rangle$, respectively, are orthogonal and make equal angles of $\pi/8$ with the nonorthogonal signal states $|u\rangle$ and $|v\rangle$, respectively. The target qubit entering the target port of the CNOT gate consists of the two orthonormal linearly-polarized photon polarization basis states $|w_a\rangle$ and $|w_b\rangle$ of the probe. When $|e_0\rangle$ enters the control port, $\{|w_a\rangle, |w_b\rangle\}$ becomes $\{|w_b\rangle, |w_a\rangle\}$, and when $|e_1\rangle$ enters the control port, $\{|w_a\rangle, |w_b\rangle\}$ remains the same. The initial unnormalized target state of the probe can, in this case, be shown to be given by (See Fig. 3 of [1]):

$$|A_2\rangle = (1-2E)^{1/2}|w_a\rangle + (2E)^{1/2}|w_b\rangle, \tag{12}$$

and the unnormalized transition state is given by

$$|A_1\rangle = (1-2E)^{1/2}|w_a\rangle - (2E)^{1/2}|w_b\rangle. \tag{13}$$

Next, by arguments directly paralleling those of [1], using Eqs.(7)-(10), one has the following correlations between the signal states and the projected probe states, $|\sigma_+\rangle$ and $|\sigma_-\rangle$:

$$|u\rangle \iff |\sigma_+\rangle, \quad |\bar{u}\rangle \iff |\sigma_-\rangle, \tag{14}$$

and

$$|v\rangle \iff |\sigma_-\rangle\,, \quad |\bar{v}\rangle \iff |\sigma_+\rangle\,. \tag{15}$$

The measurement basis for the symmetric von Neumann projective measurement of the probe must be orthogonal and symmetric about the correlated probe states, $|\sigma_+\rangle$ and $|\sigma_-\rangle$, in the two-dimensional Hilbert space of the probe [1]. Thus, consistent with Eqs.(2) and (3), I define the following orthonormal measurement basis states:

$$|w_+\rangle = 2^{-1/2}(|w_a\rangle + |w_b\rangle), \tag{16}$$

$$|w_-\rangle = 2^{-1/2}(|w_a\rangle - |w_b\rangle). \tag{17}$$

Next, one notes that the correlations of the projected probe states $|\sigma_+\rangle$ and $|\sigma_-\rangle$ with the measurement basis states $|w_+\rangle$ and $|w_-\rangle$ are indicated, according to Eqs.(2), (3), (16), and (17), by the following probabilities:

$$\frac{|\langle w_+|\sigma_+\rangle|^2}{|\sigma_+|^2} = \frac{|\langle w_-|\sigma_-\rangle|^2}{|\sigma_-|^2} = \frac{1}{2} - \frac{E^{1/2}(1-2E)^{1/2}}{(1-E)}, \tag{18}$$

$$\frac{|\langle w_+|\sigma_-\rangle|^2}{|\sigma_-|^2} = \frac{|\langle w_-|\sigma_+\rangle|^2}{|\sigma_+|^2} = \frac{1}{2} + \frac{E^{1/2}(1-2E)^{1/2}}{(1-E)}, \tag{19}$$

consistent with Eqs.(198) and (199) of [1], and implying the following dominant state correlations:

$$|\sigma_+\rangle \iff |w_-\rangle\,, \quad |\sigma_-\rangle \iff |w_+\rangle\,. \tag{20}$$

Next combining the correlations (14), (15), and (20), one thus establishes the following correlations:

$$\{|u\rangle\,, |\bar{v}\rangle\} \iff |\sigma_+\rangle \iff |w_-\rangle\,, \tag{21}$$

$$\{|\bar{u}\rangle\,, |v\rangle\} \iff |\sigma_-\rangle \iff |w_+\rangle\,, \tag{22}$$

to be implemented by the projective measurement of the probe, as in [1].

One therefore arrives at the following alternative entangling probe design. An incident photon coming from the legitimate transmitter is received by the probe in one of the four signal-photon linear-polarization states $|u\rangle$, $|\bar{u}\rangle$, $|v\rangle$, or $|\bar{v}\rangle$ in the BB84 protocol. The signal photon enters the control port of a CNOT gate. The initial state of the probe is a photon in linear-polarization state $|A_2\rangle$ entering the target port of the CNOT gate. The probe photon is produced by a single-photon source and is appropriately timed with reception of the signal photon by first sampling a few successive signal pulses to determine the repetition rate of the transmitter. The photon linear-polarization state $|A_2\rangle$, according to Eq.(12), is given by

$$|A_2\rangle = (1-2E)^{1/2}\,|w_a\rangle + (2E)^{1/2}\,|w_b\rangle\,, \tag{23}$$

and can be simply set for an error rate E by means of a polarizer. In this way the entangling probe can be tuned to the chosen error rate to be induced by the probe. The outgoing gated signal photon is relayed on to the legitimate receiver, and the gated probe photon enters a Wollaston prism, oriented to separate photon orthogonal-linear-polarization states $|w_+\rangle$ and $|w_-\rangle$, and the photon is then detected by one of two photodetectors. This is an ordinary von Neumann projective measurement. If the basis, revealed during the public basis-reconciliation phase of the BB84 protocol, is $\{|u\rangle,\ |\bar{u}\rangle\}$, then the photodetector located to receive the polarization state $|w_-\rangle$ or $|w_+\rangle$, respectively, will indicate, in accord with the correlations (21) and (22), that a state $|u\rangle$ or $|\bar{u}\rangle$, respectively, was most likely measured by the legitimate receiver. Alternatively, if the announced basis is $\{|v\rangle,\ |\bar{v}\rangle\}$, then the photodetector located to receive the polarization state $|w_+\rangle$ or $|w_-\rangle$, respectively, will indicate, in accord with the correlations (21) and (22), that a state $|v\rangle$ or $|\bar{v}\rangle$, respectively, was most likely measured by the legitimate receiver. By comparing the record of probe photodetector triggering with the sequence of bases revealed during reconciliation, then the likely sequence of ones and zeroes constituting the key, prior to privacy amplification, can be assigned. In any case the net effect is to yield, for a set error rate E, the maximum information gain to the probe, which is given by Eq.(11).

4 POVM MEASUREMENT OF ENTANGLING PROBE

Instead of performing a von-Neumann projective measurement of the entangling probe (using the Wollaston prism along with two photodetectors, as in the above), one can conclusively detect the two nonorthogonal probe states $|\sigma_+\rangle$ and $|\sigma_-\rangle$, at least some of the time. For this purpose, the POVM receiver (See Fig.1 of [4]) must simply be set up to distinguish the nonorthogonal states $|\sigma_+\rangle\,/\,|\sigma_+|$ and $|\sigma_-\rangle\,/\,|\sigma_-|$ (instead of the states $|u\rangle$ and $|v\rangle$ described in [4]). For this purpose, the Wollaston prism in Fig.1 of [4] must be aligned to separate the nonorthogonal states:

$$\left|\hat{e}_{\sigma_+ + \sigma_-}\right\rangle \equiv \frac{\frac{|\sigma_+\rangle}{|\sigma_+|} + \frac{|\sigma_-\rangle}{|\sigma_-|}}{\left[\left(\frac{\langle\sigma_+|}{|\alpha_+|} + \frac{\langle\sigma_-|}{|\sigma_-|}\right)\left(\frac{|\sigma_+\rangle}{|\sigma_+|} + \frac{|\sigma_-\rangle}{|\sigma_-|}\right)\right]^{1/2}} \tag{24}$$

and

$$\left|\hat{e}_{\sigma_+ - \sigma_-}\right\rangle \equiv \frac{\frac{|\sigma_+\rangle}{|\sigma_+|} - \frac{|\sigma_-\rangle}{|\sigma_-|}}{\left[\left(\frac{\langle\sigma_+|}{|\alpha_+|} - \frac{\langle\sigma_-|}{|\sigma_-|}\right)\left(\frac{|\sigma_+\rangle}{|\sigma_+|} - \frac{|\sigma_-\rangle}{|\sigma_-|}\right)\right]^{1/2}} \tag{25}$$

(instead of $\left|\hat{e}_{u+v}\right\rangle$ and $\left|\hat{e}_{u-v}\right\rangle$, as in [4]). The inconclusive rate $R_?$ (or, equivalently, $P_?$ in the notation of [4]) of the POVM receiver is given by [4], [9]

$$R_? = \frac{\langle\sigma_+|\sigma_-\rangle}{|\sigma_+|\,|\sigma_-|}. \tag{26}$$

Next, using Eqs.(2) and (3) in Eq.(26) and solving for E, one obtains

$$E = \frac{1 - R_?}{3 - R_?}. \tag{27}$$

For this case of measurement of the probe with the POVM receiver, according to Eq.(27), E can be treated as a parameter ranging from 0 to 1/3 and determined by a set inconclusive rate $R_?$. The conclusive rate R_c is given by

$$R_c = 1 - R_? \; . \tag{28}$$

The overlap Q between the states $|\sigma_+\rangle$ and $|\sigma_-\rangle$ is given by

$$Q = \frac{\langle\sigma_+|\sigma_-\rangle}{|\sigma_+|\,|\sigma_-|}, \tag{29}$$

or using Eqs.(26), one obtains

$$Q = R_?. \tag{30}$$

Also, substituting Eq.(27) in Eq.(23), one obtains

$$|A_2\rangle = (1 + R_?)^{1/2}\,|w_a\rangle + 2^{1/2}(1 - R_?)^{1/2}\,|w_b\rangle\,, \tag{31}$$

in which, since $|A_2\rangle$ is not normalized, an overall factor of $(3{-}R_?)^{-1/2}$, appearing in both $|A_2\rangle$ and $|A_1\rangle$, is dropped. Analogously , one obtains

$$|A_1\rangle = (1 + R_?)^{1/2}\,|w_a\rangle - 2^{1/2}(1 - R_?)^{1/2}\,|w_b\rangle\,. \tag{32}$$

According to Eq.(31), the initial state $|A_2\rangle$ of the probe can be tuned to a set inconclusive rate of the POVM receiver. The reflection coefficient R_1 of the beamsplitter BS_1 in the POVM-receiver in Fig. 1 of [4] must, for the case at hand, be given by

$$R_1 = \tan^2\left(\frac{1}{2}\cos^{-1}Q\right) = \frac{1-Q}{1+Q}, \tag{33}$$

or substituting Eq.(30) in Eq.(33), one obtains

$$R_1 = \frac{1 - R_?}{1 + R_?}. \tag{34}$$

Thus the reflection coefficient R_1 must be set, according to Eq.(34), by the set inconclusive rate. This will require a beamsplitter with an adjustable reflection coefficient.

Finally, it is important to emphasize that, if the photon loss rate, due to attenuation in the key distribution channel between the probe and the legitimate receiver, equals the inconclusive rate $R_?$, and only the conclusive states are relayed by the probe to the legitimate receiver, then the entangling probe together with the POVM receiver can obtain complete information on the pre-privacy-amplified key, once the polarization bases are announced in the public channel during reconciliation [9]. Also, to counter alteration in the attenuation due to the probe, the legitimate channel may be replaced by a more transparent one [10]. One may therefore conclude that the BB84 protocol has a vulnerability very similar to the well-known vulnerability of the B92 (Bennett 1992) protocol [9], [10]. It is also important to emphasize that, because for the present implementation one has $0 \leq E \leq 1/3$, the inconclusive rate, according to Eq.(27), can range here from 0 to 1, and can match a corresponding loss rate in the channel connecting the probe to the legitimate receiver. If the inconclusive rate $R_?$ is chosen to match the loss rate in the channel connecting to the legitimate receiver, then the initial state of the probe must be tuned (using a polarizer located between the single-photon source and the target entrance port of the CNOT gate) to the value given by Eq.(31).

5 CONCLUSION

The design is determined for an optimized quantum cryptographic entangling probe attacking the BB84 protocol of QKD and yielding maximum information to the probe for a full range of induced error rates. Also, it is demonstrated that if the projective measurement of the probe is replaced by a POVM receiver, the measurements are conclusive, at least some of the time, for a full range of inconclusive rates.

6 ACKNOWLEDGEMENTS

This work was supported by the U.S. Army Research Laboratory and the Defense Advanced Research Projects Agency.

References

[1] H. E. Brandt, “Quantum cryptographic entangling probe,” Phys. Rev. A **71**, 042312(14) (2005).

[2] H. E. Brandt, ”Design for a quantum cryptographic entangling probe,” J. Modern Optics (2005).

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.

[4] H. E. Brandt, ”Positive operator valued measure in quantum information processing,” Am. J. Phys. **67**, 434-439 (1999).

[5] H. E. Brandt, “Qubit devices and the issue of quantum decoherence,” Prog. Quantum Electron. **22**, 257-370 (1998).

[6] H. E. Brandt and J. M. Myers, US Patent No. 5,999,285 (7 December 1999).

[7] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, “Aspects of entangled translucent eavesdropping in quantum cryptography,” Phys. Rev. A **56**, 4456-4465 (1997); Erratum, **58**, 2617 (1998).

[8] J. M. Myers and H. E. Brandt, “Converting a positive operator-valued measure to a design for a measuring instrument on the laboratory bench,” Meas. Sci. Technol. **8**, 1222-1227 (1997).

[9] H. E. Brandt, ”Conclusive eavesdropping in quantum key distribution,” J. Opt. B: Quantum Semiclass. Opt. **7** (2005)

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, ”Quantum Cryptography,” Rev. Mod. Phys. **74**, 145-195 (2002) (see p. 152).